FINAL This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSMC.2021.3117742, IEEE Transactions on Systems, Man, and Cybernetics: Systems.

Proportional-Integral Observer Design for Uncertain Time-Delay Systems Subject to Deception Attacks: An Outlier-Resistant Approach

Di Zhao, Zidong Wang, Qing-Long Han and Guoliang Wei

***Abstract*—This paper deals with the proportional-integral observer (PIO) design problem for a class of linear systems with distributed time-delays and randomly occurring parameter uncertainties. The measurement signals, transmitted from the sensors to the observer, might suffer from the randomly occurring deception attacks. The random occurrences of parameter uncertainties and deception attacks are governed by two series of Bernoulli random variables with known probability distributions. An outlier-resistant PIO is developed by introducing an innovation saturation mechanism for the sake of alleviating the adverse effects induced by the deception attacks on the estimation performance. The purpose of the addressed problem is to design a PIO that is capable of guaranteeing the mean-square boundedness of the estimation errors while achieving the desired security level. The desired PIO gain is designed by solving a matrix inequality and the validity of the results obtained is shown by a numerical simulation example.**

***Index Terms*—Proportional-integral observer, outlier-resistant state estimation, randomly occurring deception attacks, randomly occurring parameter uncertainties, distributed time-delays.**

I. Introduction

As early as in the seventies, the proportional-integral observer (PIO) has been constructed in [40] by introducing an extra integral operation with respect to the output estimation error into the traditional Luenberger observer. Hitherto, the PIO has shown great potential in a diverse range of practical domains such as manufacturing processes, network communication systems, power circuit systems and economic systems [3], [5]. Briefly speaking, the PIO consists of the proportional term and the integral term with respect to the output estimation error, thereby reflecting the current and historical information for achieving better performance as compared with the traditional Luenberger observer. Thanks to the utilization of integral action, the PIO has exhibited promising advantages in improving the system robustness, eliminating the steady-state error as well as increasing the observer design freedom. Accordingly, considerable research attention has been paid to the PIO design issue with fruitful results available in the literature, see e.g. [9], [21], [22], [31], [33], [34].

Time-delays, which are known to have substantial impacts on system performance, are often encountered in many real systems (e.g. aerospace systems, industrial control systems, telemedicine system, robot teleoperation system and network communication systems) for a variety of reasons such as equipment aging and complicated structure. In the past few decades, there has been an enormous research effort into the investigation on various kinds of time-delays including constant delays, time-varying delays, random delays, and distributed delays [19], [20], [27], [39], [46]. Apart from the time-delay phenomena, parameter uncertainties serve as another main factor that complicates the system analysis and synthesis [4], [25], [28], [37]. In today's networked world, parameter uncertainties may take place in a random way due probably to network-induced random faults, sudden environmental disturbances and unpredictable fluctuations of network load. Such kind of uncertainties is customarily referred to as randomly occurring parameter uncertainties (ROPUs) which, together with time-delays, may result in undesirable dynamic behaviors such as oscillation, chaos or even divergence. Therefore, it is of great importance to make dedicated efforts in disposing of the influence from time-delays and/or ROPUs on the system analysis and synthesis [26], [45].

With the rapid advancement of networking technologies, networked systems (NSs) has become an emerging research frontier in the past few decades [7], [8], [10], [13], [15], [23], [29]. In practical applications of NSs, it is a normal practice for the system components (such as controllers, sensors, estimators and actuators) to be connected through shared network media, thereby achieving remote, reliable, real-time yet collaborative operation and control. Because of the inherent openness of the shared communication channel, NSs are vulnerable to miscellaneous cyber-threats, and some representative examples found in the real world include Regin malware threat, Operation Aurora, Petya Ransomware, and DigiNotar hacker incident, to name a few. As a result, particular research interest has been gained to develop appropriate estimation/control schemes to improve the system security and relieve the negative effects caused by cyber-attacks on the

This work was supported in part by the National Natural Science Foundation of China under Grants 61873148, 61873169 and 61933007, the Royal Society of the U.K., and the Alexander von Humboldt Foundation of Germany.
(Corresponding author: Guoliang Wei.)

D. Zhao is with the College of Science, the Biomedical Engineering Postdoctoral Research Mobile Station, University of Shanghai for Science and Technology, Shanghai 200093, China. (Email: zhaodi0907520@163.com).

Z. Wang is with the Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom. (Email: zidong.Wang@brunel.ac.uk).

Q.-L. Han is with the School of Science, Computing and Engineering Technologies, Swinburne University of Technology, Melbourne, VIC 3122, Australia. (Email: qhan@swin.edu.au).

G. Wei is with the College of Science, University of Shanghai for Science and Technology, Shanghai 200093, China. (Email: guoliang.wei@usst.edu.cn).

system performance [11], [32], [42]. For example, in [6], [8], [17], [47], the security control problems have been investigated for systems under cyber-attacks, and the security-guaranteed estimation schemes have been developed in [14], [35], [41].

In general, the common cyber-attacks can be classified as denial of service attacks and deception attacks in terms of the ways they are implemented, and the deception attacks are known to be comparatively dangerous due to their behaviors of data hijacking and falsification. When launching deception attacks, the adversaries capture the data packets and inject the false information (or IP address) to deliberately prevent the system operation from normal execution, thus destroying hardware/software and even crashing the whole system. On the other hand, the intended cyber-attacks sent by the adversaries might *not* be always successful on account of various reasons such as 1) deployment of the detection software and protection equipment; 2) inherent bandwidth limit of the shared communication channel; and 3) network-induced phenomena such as packet losses, communication delays and channel fading, and all these have led to the random nature of the deception attacks. As such, it is practically meaningful to model the NS-based deception attacks as random events obeying certain distributions, and such a modeling strategy has been adopted in quite a few recent results, see e.g. [24], [36], [44] where the deception attacks have been assumed to be regulated by Bernoulli/Markov process with known probability distributions.

It is worth noting that, due to effects of the deception attacks, the measurement outputs might undergo abrupt yet large disturbances which, in turn, might induce the so-called *measurement outliers* contributing further to the deterioration of the estimation performance. In other words, it is quite likely that the measurement outliers, if not adequately tackled, would give rise to abnormal changes of the innovation values in the state estimator, thereby jeopardizing the estimation accuracy. As such, it becomes necessary to develop an estimator that is insensitive/invulnerable to the measurement outliers, and such an estimator is termed as the *outlier-resistant* estimator. Recently, the outlier-resistant state estimation issue has begun to arouse initial research interest with some elegant results, see e.g. [2], [12], [30], [38], [48]. For instance, a Kalman filter with saturated output injection has been constructed in [16] to withstand the measurement outliers, and the outlier-resistant state estimation issue has been discussed in [1] for a class of linear time-invariant systems in the presence of measurement outliers. Nonetheless, a thorough literature search has exhibited that the relevant results for the outlier-resistant PIO design issues have been really scattered due primarily to the analytical complexity induced by the integral term in PIO, and this motivates our current investigation.

Inspired by the above discussions, the focus of this paper is on the design of the outlier-resistant PIO for a class of discrete-time delayed systems with ROPUs subject to randomly occurring deception attacks (RODAs). In doing so, we are confronted with the following three fundamental challenges: 1) how to establish a suitable theoretical framework to handle the analytical complexity brought by the random occurrences of the parameter uncertainties and the deception attacks? 2) how to develop a reliable scheme to deal with the measurement outliers induced by the deception attacks? and 3) how to construct an appropriate criteria to quantify the combined impact caused by the RODAs and the stochastic noises on the estimation errors? As such, the objective of this paper is to conquer the three challenges. The main technical contributions lie in that: *1) the PIO design issue is, for the first time, addressed for a kind of discrete-time delayed system subject to RODAs; 2) an innovation-saturation-based mechanism is employed in the PIO design to alleviate the impacts from the deception attacks on the estimation errors; and 3) sufficient conditions are derived to ensure the exponentially mean-square (EMS) boundedness and further achieve the desired security level.*

The rest of this paper is organized as follows. The outlier-resistant PIO design issue is formulated for the discrete-time delayed systems subject to RODAs in Section II. In Section III, the EMS boundedness of the estimation errors is analyzed and a sufficient condition for security is provided. Subsequently, the expected outlier-resistant PIO is designed by using the linear matrix inequality (LMI) method. Section IV presents a numerical example to verify the usefulness and advantage of the proposed PIO design scheme, and some conclusions are drawn in Section V.

Notation. For notational convenience, $\mathbb{R}^{n\times m}$ and $\mathbb{R}^n$ are, respectively, used to denote the set of all $n\times m$ real matrices and the n-dimensional Euclidean space. $X<Y$ (respectively, $X\leq Y$) implies that $Y-X$ is positive definite (respectively, positive semi-definite), where X and Y are real symmetric matrices. I_q stands for a q-dimensional identity matrix and the Kronecker product is denoted by the symbol "$\otimes$". In addition, $\lambda_{\min}(Z)$ and $\lambda_{\max}(Z)$ are, respectively, the minimum and maximum eigenvalues of the symmetric matrix Z.

II. Problem Formulation and Preliminaries

A. The System Model

Consider a class of linear discrete time-delayed systems with ROPUs:

$$\begin{cases} x(s+1) = \big(A+\kappa(s)B(s)\big)x(s)+Mw(s) \\ \qquad\qquad + H\displaystyle\sum_{h=1}^{\hbar}\ell_h x(s-h) \\ y(s) = Cx(s) \\ z(s) = Dx(s) \\ x(\jmath) = \phi(\jmath), \quad \forall \jmath\in\mathfrak{H}\triangleq\{-\hbar,\ldots,-1,0\} \end{cases} \tag{1}$$

where $x(s)\in\mathbb{R}^{n_x}$, $y(s)\in\mathbb{R}^{n_y}$, and $z(s)\in\mathbb{R}^{n_z}$ are, respectively, the state, the measurement output and the output to be estimated; $\hbar$ is a given positive integer and ℓ_h is a positive scalar; $\phi(\jmath)$ is the initial condition sequence; A, C, D, M and H are given matrices with compatible dimensions. $w(s)\in\mathbb{R}$ possesses the following statistical properties:

$$\mathbb{E}\{w(s)\}=0, \quad \mathbb{E}\{w(p)w(q)\}=\begin{cases}\vartheta_w^2, & \text{if } p=q\\ 0, & \text{if } p\neq q\end{cases} \tag{2}$$

where ϑ_w is a known scalar.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSMC.2021.3117742, IEEE Transactions on Systems, Man, and Cybernetics: Systems.

The random variable $\kappa(s)$ is a Bernoulli-distributed sequence satisfying

$$\text{Prob}\{\kappa(s)=1\}=\bar{\kappa}, \quad \text{Prob}\{\kappa(s)=0\}=1-\bar{\kappa}$$

where $\bar{\kappa}\in[0,1)$ is a constant that is known a priori.

The real matrix $B(s)$, which accounts for the parameter uncertainty, meets the following constraint:

$$B(s)=RS(s)T \tag{3}$$

where matrices R and T are known, $S(s)\in\mathbb{R}^{n_s\times n_s}$ is an unknown matrix function satisfying

$$S^T(s)S(s)\leqslant I. \tag{4}$$

B. The Cyber-Attack Model

In the current investigation, the measurement signals are transmitted to the observer via a shared communication network, where the data transmission might be maliciously falsified through the RODAs expressed by

$$\upsilon(s)=y(s)+\vartheta(s)\varpi(s). \tag{5}$$

Here, $\upsilon(s)\in\mathbb{R}^{n_y}$ denotes the input signal of the observer that is corrupted by the attackers, $\varpi(s)\in\mathbb{R}^{n_y}$ denotes the deception attack sent by the hostile attackers and is characterized by

$$\varpi(s)=-y(s)+\delta(s) \tag{6}$$

with $\delta(s)\neq 0$ being an arbitrary signal. $\vartheta(s)$ is a Bernoulli random variable regulating the RODAs with the following probability distribution:

$$\text{Prob}\{\vartheta(s)=1\}=\bar{\vartheta}, \quad \text{Prob}\{\vartheta(s)=0\}=1-\bar{\vartheta}$$

where $\bar{\vartheta}\in[0,1)$ is a known constant. Without loss of generality, $\vartheta(s)$, $\kappa(s)$ and $w(s)$ are assumed to be uncorrelated.

Remark 1: In practical engineering, deception attacks sent by the adversaries cannot be always successful because of the anti-attack countermeasures (e.g. deployment of the defense devices or detectors) and the limited communication capacity. In this sense, from the defender's perspective, the deception attacks take place in a random manner obeying a Bernoulli sequence with certain statistical property. In accordance with (5), if the deception attack is successful, i.e. $\vartheta(s)=1$, the actual signal received by the observer is $\delta(s)$, which means that the measurement outlier is injected to the observer. If the deception attack is unsuccessful, i.e. $\vartheta(s)=0$, the actual signal received by the observer is $y(s)$, which indicates that the normal measurement signals are transmitted to the observer. Note that the probability of successful deception attacks $\bar{\vartheta}$ can be identified *a priori* via some statistical experiments.

C. The Outlier-Resistant PIO

For restraining the estimation performance from being distorted by the RODAs, a saturation function is *purposely* introduced when handling the observer design issue. Specifically, the outlier-resistant PIO is proposed as follows:

$$\begin{cases}\hat{x}(s+1)=A\hat{x}(s)+H\sum_{h=1}^{\hbar}\ell_h\hat{x}(s-h)\\ \qquad\qquad +F_P\Im\big(\upsilon(s)-C\hat{x}(s)\big)+F_I\chi(s)\\ \chi(s+1)=\chi(s)+F\Im\big(\upsilon(s)-C\hat{x}(s)\big)\\ \hat{z}(s)=D\hat{x}(s)\\ \chi(0)=0\\ \hat{x}(\jmath)=0, \quad \forall\jmath\in\mathfrak{H}\end{cases} \tag{7}$$

where $\hat{x}(s)\in\mathbb{R}^{n_x}$ is $x(s)$'s estimation, $\hat{z}(s)\in\mathbb{R}^{n}$ is $z(s)$'s estimation, and $\chi(s)\in\mathbb{R}^{n_\chi}$ describes the integral of the weighted output estimation error. Here, F_P, F_I and F are the observer parameters to be determined.

Define the saturation function $\Im(\cdot):\mathbb{R}^{n_y}\to\mathbb{R}^{n_y}$ as

$$\Im(l)=\begin{bmatrix}\Im(l_1) & \Im(l_2) & \cdots & \Im(l_{n_y})\end{bmatrix}^T, \quad \forall l\in\mathbb{R}^{n_y} \tag{8}$$

where $\Im(l_q)=\text{sign}(l_q)\min\{l_q^M, |l_q|\}$ and l_q^M is the qth entry of saturation level vector l^M ($q\in\mathfrak{Y}\triangleq\{1,2,\ldots,n_y\}$). Moreover, the saturation function $\Im(\cdot)$ is a sector-bounded nonlinear function satisfying:

$$\big(\Im(\alpha_q)-\mu_q\alpha_q\big)^T\big(\Im(\alpha_q)-\alpha_q\big)\leqslant 0, \quad (q\in\mathfrak{Y}) \tag{9}$$

where α_q is a given scalar and μ_q is a positive scalar satisfying $0<\mu_q<1$.

Remark 2: Different from the conventional PIO, the outlier-resistant PIO constructed in (7) contains an intentionally introduced saturation constraint on the innovations and, accordingly, the measurement outliers (induced by the deception attacks) could be adequately tackled. Specifically, the innovation in the outlier-resistant PIO (7) can be constrained within a predetermined range owing to the saturation function (8), where the saturation level l^M is dependent on the prior knowledge (on the range of the innovation and the tolerance level of the detector). In this case, the outlier-resistant PIO would be more effective than the conventional PIO in alleviating the negative effects of the deception attacks on the estimation errors. In fact, the outlier-resistant PIO specializes to the conventional PIO when the saturation level l^M approaches infinity.

Denoting $\tilde{x}(s)\triangleq x(s)-\hat{x}(s)$ and $\tilde{z}(s)\triangleq z(s)-\hat{z}(s)$, the dynamics of the estimation errors can be written as

$$\begin{cases}\tilde{x}(s+1)=A\tilde{x}(s)+H\sum_{h=1}^{\hbar}\ell_h\tilde{x}(s-h)+\kappa(s)B(s)x(s)\\ \qquad\qquad -F_P\Im\big(\upsilon(s)-C\hat{x}(s)\big)-F_I\chi(s)+Mw(s)\\ \chi(s+1)=\chi(s)+F\Im\big(\upsilon(s)-C\hat{x}(s)\big)\\ \tilde{z}(s)=D\tilde{x}(s)\\ \chi(0)=0\\ \tilde{x}(\jmath)=\phi(\jmath), \quad \forall\jmath\in\mathfrak{H}\end{cases} \tag{10}$$

Setting $\psi(s)\triangleq\begin{bmatrix}x^T(s) & \tilde{x}^T(s) & \chi^T(s)\end{bmatrix}^T$, the following augmented system is obtained:

$$\begin{cases} \psi(s+1) = \big(\mathcal{A} + \bar{\kappa}\mathcal{B}(s) + \tilde{\kappa}(s)\mathcal{B}(s)\big)\psi(s) \\ \qquad + \mathcal{H}\sum_{h=1}^{\hbar}\ell_h\psi(s-h) + \mathcal{M}w(s) \\ \qquad + \mathcal{F}\Im\big(\zeta(s)\big) \\ \psi(\jmath) = \varphi(\jmath), \quad \forall \jmath \in \mathfrak{H} \end{cases} \tag{11}$$

where $\varphi(\jmath) \triangleq \begin{bmatrix}\phi^T(\jmath) & \phi^T(\jmath) & 0\end{bmatrix}^T$ and

$$\mathcal{A} \triangleq \begin{bmatrix} A & 0 & 0 \\ 0 & A & -F_I \\ 0 & 0 & I \end{bmatrix}, \ \mathcal{H} \triangleq \begin{bmatrix} H & 0 & 0 \\ 0 & H & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\mathcal{B}(s) \triangleq \begin{bmatrix} B(s) & 0 & 0 \\ B(s) & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\mathcal{M} \triangleq \begin{bmatrix} M \\ M \\ 0 \end{bmatrix}, \quad \tilde{\kappa}(s) \triangleq \kappa(s) - \bar{\kappa}$$

$$\mathcal{F} \triangleq \begin{bmatrix} 0 \\ -F_P \\ F \end{bmatrix}, \quad \tilde{\vartheta}(s) \triangleq \vartheta(s) - \bar{\vartheta}$$

$$\zeta(s) \triangleq \big(\mathcal{C}_1 + \tilde{\vartheta}(s)\mathcal{C}_2\big)\psi(s) + \big(\bar{\vartheta} + \tilde{\vartheta}(s)\big)\delta(s)$$

$$\mathcal{C}_1 \triangleq \begin{bmatrix} -\bar{\vartheta}C & C & 0 \end{bmatrix}, \ \mathcal{C}_2 \triangleq \begin{bmatrix} -C & 0 & 0 \end{bmatrix}.$$

For facilitating the subsequent analysis, the definitions of EMS boundedness and mean-square security are given as follows.

Definition 1: The compacted system (11) is exponentially ultimately bounded in mean-square sense if the system dynamics $\psi(s)$ is constrained by

$$\mathbb{E}\{\|\psi(s)\|^2\} \leqslant \epsilon^s\alpha + \nu(s) \text{ and } \lim_{s\to+\infty}\nu(s) = \bar{\nu}. \tag{12}$$

where ϵ, α and $\bar{\nu}$ are constants satisfying $0 < \epsilon < 1$, $\alpha > 0$ and $\bar{\nu} > 0$.

Definition 2: The augmented system (11) is mean-square ς-secure if the following two conditions are satisfied simultaneously: a) the augmented system (11) is exponentially ultimately bounded in mean-square sense; and b) the system dynamics $\psi(s)$ is governed by

$$\mathbb{E}\{\|\psi(s)\|^2\} \leqslant \varsigma, \quad \forall k \geqslant 0, \tag{13}$$

where ς is a given positive scalar denoting the desired security level.

Remark 3: In this paper, the concept of EMS boundedness presented in Definition 1 is employed to depict the joint influence from the RODAs and the stochastic noise on the estimation errors, and the concept of mean-square security presented in Definition 2 is used to characterize the ability of the NSs to tolerate adversaries and recover from cyber-attacks. Obviously, if the augmented system (11) is exponentially ultimately bounded in mean-square sense, then it must be mean-square ς-secure.

The objective of this paper is to design an outlier-resistant PIO (7) for system (1) subject to RODAs.

III. Main Results

In this section, we are going to design an outlier-resistant PIO for the system (1) subject to RODAs. Sufficient conditions are provided to guarantee the EMS boundedness of the estimation errors and the mean-square security is simultaneously satisfied. Then, the desired PIO gains are parameterized in terms of the solution to an LMI.

The following lemmas are given to facilitate the sequel development.

Lemma 1: The saturation function $\Im\big(\zeta(s)\big)$ in (11) satisfies

$$\begin{aligned} &\Im^T\big(\zeta(s)\big)\Im\big(\zeta(s)\big) + \zeta^T(s)U^T\zeta(s) \\ &- \zeta^T(s)(U^T + I)\Im\big(\zeta(s)\big) \leqslant 0 \end{aligned} \tag{14}$$

where $U \triangleq \mathrm{diag}\{\mu_1, \mu_2, \ldots, \mu_q\}$.

Proof: From (9), it is easy to verify that

$$\begin{aligned} &\big(\Im(l) - Ul\big)^T\big(\Im(l) - l\big) \\ =&\sum_{q=1}^{n_y}\Big(\big(\Im(\alpha_q) - \mu_q\alpha_q\big)^T\big(\Im(\alpha_q) - \alpha_q\big)\Big) \\ \leqslant& 0. \end{aligned} \tag{15}$$

By letting $l = \zeta(s)$, we have

$$\Big(\Im(\zeta(s)) - U\zeta(s)\Big)^T\Big(\Im(\zeta(s)) - \zeta(s)\Big) \leqslant 0$$

which implies that inequality (14) holds. ■

Lemma 2: Let $z(s) \in \mathbb{R}^{n_z}$ ($n_z = 2n_x + n_\chi$), $Z \in \mathbb{R}^{n_z\times n_z}$ be a positive semi-definite matrix, $b_h > 0$ ($h = 1, 2, \ldots, \hbar$) be scalar constants, and $\hbar$ be a positive integer. The following relationship is true:

$$\begin{aligned} &\left(\sum_{h=1}^{\hbar}b_hz(s)\right)^T Z\left(\sum_{h=1}^{\hbar}b_hz(s)\right) \\ \leqslant&\left(\sum_{h=1}^{\hbar}b_h\right)\sum_{h=1}^{\hbar}b_hz^T(s)Zz(s). \end{aligned} \tag{16}$$

Lemma 3: Let $X = X^T$, Y and W be real matrices of appropriate dimensions, and $G(s)$ satisfies $G^T(s)G(s) \leqslant I$. Then

$$X + YG(s)W + W^TG^T(s)Y^T < 0 \tag{17}$$

if and only if there exists a positive scalar π such that

$$X + \pi YY^T + \frac{1}{\pi}W^TW < 0 \tag{18}$$

or

$$\begin{bmatrix} X & \pi Y & W^T \\ \pi Y^T & -\pi I & 0 \\ W & 0 & -\pi I \end{bmatrix} < 0. \tag{19}$$

A. Security Analysis

In this subsection, we shall analyze the EMS boundedness of the estimation errors and derive a sufficient condition to guarantee the ς-security of (11).

Theorem 1: Let the observer parameters F_P, F_I and F be given. If there exist positive definite matrices P, Q and positive scalar ι satisfying

$$\Omega = \begin{bmatrix} \Omega_1 & \star \\ \Omega_2 & \Omega_3 \end{bmatrix} < 0 \tag{20}$$

and

$$\frac{\bar{\ell}\lambda_{\max}(Q)\hbar(\varepsilon^{\hbar}-1)+(\hbar+1)\bar{\lambda}}{\lambda_{\min}(P)\varepsilon^{\rho}}\sup_{\jmath\in\mathfrak{H}}\mathbb{E}\{\|\varphi(\jmath)\|^2\} + \frac{\varepsilon}{\lambda_{\min}(P)(\varepsilon-1)}\beta \leqslant \varsigma. \tag{21}$$

where

$$\Omega_1 \triangleq \begin{bmatrix} \Omega_1^{11} & \star & \star & \star \\ 0 & \Omega_1^{22} & \star & \star \\ \Omega_1^{31} & 0 & \Omega_1^{33} & \star \\ \Omega_1^{41} & 0 & \Omega_1^{43} & \Omega_1^{44} \end{bmatrix}$$

$$\Omega_2 \triangleq \begin{bmatrix} \mathcal{A}+\bar{\kappa}\mathcal{B}(s) & \mathcal{H} & \mathcal{F} & 0 \end{bmatrix}, \quad \bar{\ell} \triangleq \sum_{h=1}^{\hbar}\ell_h$$

$$\Omega_3 \triangleq -P^{-1}, \quad \bar{\lambda} \triangleq \max\{\lambda_{\max}(P), \bar{\ell}\lambda_{\max}(Q)\}$$

$$\Omega_1^{11} \triangleq -P+\bar{\ell}Q-\iota\mathcal{C}_1^T U^T\mathcal{C}_1-\iota(\bar{\vartheta}-\bar{\vartheta}^2)\mathcal{C}_2^T U^T\mathcal{C}_2$$

$$\Omega_1^{22} \triangleq -\frac{1}{\bar{\ell}}Q, \quad \Omega_1^{33} \triangleq -\iota I, \quad \Omega_1^{44} \triangleq -\iota\bar{\vartheta}U^T$$

$$\Omega_1^{31} \triangleq \frac{1}{2}\iota(U^T+I)\mathcal{C}_1, \quad \Omega_1^{41} \triangleq -\iota\bar{\vartheta}U^T\big(\mathcal{C}_1+\mathcal{C}_2-\bar{\vartheta}\mathcal{C}_2\big)$$

$$\Omega_1^{43} \triangleq \frac{1}{2}\iota\bar{\vartheta}(U^T+I), \quad \beta \triangleq \lambda_{\max}(\mathcal{M}^T P\mathcal{M})\vartheta_w^2$$

and $\varepsilon > 1$ in (21) is determined by

$$\lambda_{\max}(P)(\varepsilon-1)-\gamma\varepsilon+2\bar{\ell}\lambda_{\max}(Q)\varepsilon(\varepsilon^{\hbar}-1)=0 \tag{22}$$

with

$$\gamma \triangleq \lambda_{\min}\big(-\Omega_1-\Omega_2^T P\Omega_2\big),$$

then the augmented system (11) is ς-secure in the sense of mean-square.

Proof: For examining the EMS boundedness of the augmented system (11), we construct the following Lyapunov-Krasovskii functional:

$$V\big(\psi(s)\big) = V_1\big(\psi(s)\big) + V_2\big(\psi(s)\big) \tag{23}$$

where

$$V_1\big(\psi(s)\big) \triangleq \psi^T(s)P\psi(s)$$

$$V_2\big(\psi(s)\big) \triangleq \sum_{h=1}^{\hbar}\ell_h\sum_{r=s-h}^{s-1}\psi^T(r)Q\psi(r).$$

Then, the difference of $V\big(\chi(s)\big)$ is denoted by

$$\Re V\big(\psi(s)\big) = \Re V_1\big(\psi(s)\big) + \Re V_2\big(\psi(s)\big) \tag{24}$$

where

$$\Re V_1\big(\psi(s)\big) \triangleq \mathbb{E}\{V_1\big(\psi(s+1)\big)|\psi(s)\} - V_1\big(\psi(s)\big)$$

$$\Re V_2\big(\psi(s)\big) \triangleq \mathbb{E}\{V_2\big(\psi(s+1)\big)|\psi(s)\} - V_2\big(\psi(s)\big).$$

The difference of $V_1\big(\psi(s)\big)$ along (11) is calculated by

$$\begin{aligned}
&\mathbb{E}\left\{\Re V_1\big(\chi(s)\big)\right\} \\
=&\mathbb{E}\left\{V_1\big(\psi(s+1)\big)-V_1\big(\psi(s)\big)\right\} \\
=&\mathbb{E}\bigg\{\Big(\big(\mathcal{A}+\bar{\kappa}\mathcal{B}(s)+\tilde{\kappa}(s)\mathcal{B}(s)\big)\psi(s)+\mathcal{F}\Im\big(\zeta(s)\big) \\
&+\mathcal{H}\sum_{h=1}^{\hbar}\ell_h\psi(s-h)+\mathcal{M}w(s)\Big)^T P \\
&\times\Big(\big(\mathcal{A}+\bar{\kappa}\mathcal{B}(s)+\tilde{\kappa}(s)\mathcal{B}(s)\big)\psi(s)+\mathcal{F}\Im\big(\zeta(s)\big) \\
&+\mathcal{H}\sum_{h=1}^{\hbar}\ell_h\psi(s-h)+\mathcal{M}w(s)\Big)-\psi^T(s)P\psi(s)\bigg\} \\
=&\mathbb{E}\bigg\{\psi^T(s)\Big(\mathcal{A}^T P\mathcal{A}-P+\big(\bar{\kappa}+\tilde{\kappa}(s)\big)^2\mathcal{B}^T(s)P\mathcal{B}(s) \\
&+\big(\bar{\kappa}+\tilde{\kappa}(s)\big)\mathcal{A}^T P\mathcal{B}(s)+\big(\bar{\kappa}+\tilde{\kappa}(s)\big)\mathcal{B}^T(s)P\mathcal{A}\Big)\psi(s) \\
&+\Im^T\big(\zeta(s)\big)\mathcal{F}^T P\mathcal{F}\Im\big(\zeta(s)\big)+\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)^T \\
&\times\mathcal{H}^T P\mathcal{H}\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)+w^T(s)\mathcal{M}^T P\mathcal{M}w(s) \\
&+2\Im^T\big(\zeta(s)\big)\Big(\mathcal{F}^T P\mathcal{A}+\big(\bar{\kappa}+\tilde{\kappa}(s)\big)\mathcal{F}^T P\mathcal{B}(s)\Big)\psi(s) \\
&+2\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)^T\Big(\mathcal{H}^T P\mathcal{A}+\big(\bar{\kappa}+\tilde{\kappa}(s)\big)\mathcal{H}^T \\
&\times P\mathcal{B}(s)\Big)\psi(s)+2w^T(s)\Big(\mathcal{M}^T P\mathcal{A}+\big(\bar{\kappa}+\tilde{\kappa}(s)\big) \\
&\times\mathcal{M}^T P\mathcal{B}(s)\Big)\psi(s)+2\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)^T\mathcal{H}^T \\
&\times P\mathcal{F}\Im\big(\zeta(s)\big)+2w^T(s)\mathcal{M}^T P\mathcal{F}\Im\big(\zeta(s)\big)+2w^T(s) \\
&\times\mathcal{M}^T P\mathcal{H}\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)\bigg\} \\
\leqslant&\mathbb{E}\bigg\{\psi^T(s)\Big(\mathcal{A}^T P\mathcal{A}-P+\bar{\kappa}\mathcal{B}^T(s)P\mathcal{B}(s) \\
&+\sqrt{\bar{\kappa}}\mathcal{A}^T P\mathcal{B}(s)+\sqrt{\bar{\kappa}}\mathcal{B}^T(s)P\mathcal{A}\Big)\psi(s)+\Im^T\big(\zeta(s)\big) \\
&\times\mathcal{F}^T P\mathcal{F}\Im\big(\zeta(s)\big)+\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)^T\mathcal{H}^T P\mathcal{H} \\
&\times\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)+w^T(s)\mathcal{M}^T P\mathcal{M}w(s) \\
&+2\Im^T\big(\zeta(s)\big)\Big(\mathcal{F}^T P\mathcal{A}+\sqrt{\bar{\kappa}}\mathcal{F}^T P\mathcal{B}(s)\Big)\psi(s) \\
&+2\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)^T\Big(\mathcal{H}^T P\mathcal{A}+\sqrt{\bar{\kappa}}\mathcal{H}^T P\mathcal{B}(s)\Big) \\
&\times\psi(s)+2\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)^T\mathcal{H}^T P\mathcal{F}\Im\big(\zeta(s)\big)\bigg\}.
\end{aligned} \tag{25}$$

Furthermore, in light of Lemma 2, we compute the difference of $V_2\big(\psi(s)\big)$ as follows:

$$\begin{aligned}
&\mathbb{E}\left\{\Re V_2\big(\psi(s)\big)\right\}\\
=&\mathbb{E}\left\{V_2\big(\psi(s+1)\big)-V_2\big(\psi(s)\big)\right\}\\
=&\mathbb{E}\Bigg\{\sum_{h=1}^{\hbar}\ell_h\sum_{r=s-h+1}^{s}\psi^T(r)Q\psi(r)\\
&-\sum_{h=1}^{\hbar}\ell_h\sum_{r=s-h}^{s-1}\psi^T(r)Q\psi(r)\Bigg\}\\
=&\mathbb{E}\left\{\bar{\ell}\psi^T(s)Q\psi(s)-\sum_{h=1}^{\hbar}\ell_h\psi^T(s-h)Q\psi(s-h)\right\}\\
\leqslant&\mathbb{E}\Bigg\{\bar{\ell}\psi^T(s)Q\psi(s)-\frac{1}{\bar{\ell}}\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)^T Q\\
&\times\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)\Bigg\}.
\end{aligned}\tag{26}$$

Bearing in mind the statistical characteristics of $w(s)$, we calculate the term $w^T(s)\mathcal{M}^T P\mathcal{M}w(s)$ (contained in (25)) as follows:

$$\begin{aligned}
&\mathbb{E}\{w^T(s)\mathcal{M}^T P\mathcal{M}w(s)\}\\
\leqslant&\lambda_{\max}(\mathcal{M}^T P\mathcal{M})\mathbb{E}\{w^T(s)w(s)\}=\beta.
\end{aligned}\tag{27}$$

Substituting (25)-(27) into (24) leads to

$$\begin{aligned}
&\mathbb{E}\big\{\Re V\big(\psi(s)\big)\big\}\\
=&\mathbb{E}\Big\{\Re V_1\big(\psi(s)\big)+\Re V_2\big(\psi(s)\big)\Big\}\\
\leqslant&\mathbb{E}\Bigg\{\psi^T(s)\Big(\mathcal{A}^T P\mathcal{A}-P+\bar{\kappa}\mathcal{B}^T(s)P\mathcal{B}(s)\\
&+\sqrt{\bar{\kappa}}\mathcal{A}^T P\mathcal{B}(s)+\sqrt{\bar{\kappa}}\mathcal{B}^T(s)P\mathcal{A}+\bar{\ell}Q\Big)\psi(s)\\
&+\Im^T\big(\zeta(s)\big)\mathcal{F}^T P\mathcal{F}\Im\big(\zeta(s)\big)+\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)^T\\
&\times\left(\mathcal{H}^T P\mathcal{H}-\frac{1}{\bar{\ell}}Q\right)\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)\\
&+2\Im^T\big(\zeta(s)\big)\Big(\mathcal{F}^T P\mathcal{A}+\sqrt{\bar{\kappa}}\mathcal{F}^T P\mathcal{B}(s)\Big)\\
&\times\psi(s)+2\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)^T\Big(\mathcal{H}^T P\mathcal{A}\\
&+\sqrt{\bar{\kappa}}\mathcal{H}^T P\mathcal{B}(s)\Big)\psi(s)+2\Im^T\big(\zeta(s)\big)\mathcal{F}^T P\mathcal{H}\\
&\times\left(\sum_{h=1}^{\hbar}\ell_h\psi(s-h)\right)+\beta\Bigg\}\\
=&\Im_1^T(s)\Psi_1\Im_1(s)+\beta
\end{aligned}\tag{28}$$

where

$$\Im_1(s)\triangleq\begin{bmatrix}\psi(s)\\ \sum_{h=1}^{\hbar}\ell_h\psi(s-h)\\ \Im\big(\zeta(s)\big)\end{bmatrix},\ \Psi_1\triangleq\begin{bmatrix}\Psi_1^{11} & \star & \star\\ \Psi_1^{21} & \Psi_1^{22} & \star\\ \Psi_1^{31} & \Psi_1^{32} & \Psi_1^{33}\end{bmatrix}$$

$$\begin{aligned}
\Psi_1^{11}\triangleq&-P+\bar{\ell}Q+\mathcal{A}^T P\mathcal{A}+\bar{\kappa}\mathcal{B}^T(s)P\mathcal{B}(s)\\
&+\sqrt{\bar{\kappa}}\mathcal{A}^T P\mathcal{B}(s)+\sqrt{\bar{\kappa}}\mathcal{B}^T(s)P\mathcal{A}\\
\Psi_1^{22}\triangleq&\mathcal{H}^T P\mathcal{H}-\frac{1}{\bar{\ell}}Q,\quad\Psi_1^{33}\triangleq\mathcal{F}^T P\mathcal{F}\\
\Psi_1^{21}\triangleq&\mathcal{H}^T P\mathcal{A}+\sqrt{\bar{\kappa}}\mathcal{H}^T P\mathcal{B}(s)\\
\Psi_1^{31}\triangleq&\mathcal{F}^T P\mathcal{A}+\sqrt{\bar{\kappa}}\mathcal{F}^T P\mathcal{B}(s)\\
\Psi_1^{32}\triangleq&\mathcal{F}^T P\mathcal{H}.
\end{aligned}$$

Then, it follows from Lemma 1 that

$$\begin{aligned}
&\mathbb{E}\big\{\Re V\big(\psi(s)\big)\big\}\\
\leqslant&\mathbb{E}\big\{\Im_1^T(s)\Psi_1\Im_1(s)\big\}+\beta-\iota\mathbb{E}\big\{\Im^T\big(\zeta(s)\big)\Im\big(\zeta(s)\big)\\
&+\zeta^T(s)U^T\zeta(s)-\zeta^T(s)(U^T+I)\Im\big(\zeta(s)\big)\big\}\\
=&\mathbb{E}\big\{\Im_1^T(s)\Psi_1\Im_1(s)\big\}+\beta-\iota\mathbb{E}\big\{\Im^T\big(\zeta(s)\big)\Im\big(\zeta(s)\big)\big\}\\
&-\iota\mathbb{E}\Big\{\Big(\big(\mathcal{C}_1+\tilde{\vartheta}(s)\mathcal{C}_2\big)\psi(s)+\big(\bar{\vartheta}+\tilde{\vartheta}(s)\big)\delta(s)\Big)^T U^T\\
&+\Big(\big(\mathcal{C}_1+\tilde{\vartheta}(s)\mathcal{C}_2\big)\psi(s)+\big(\bar{\vartheta}+\tilde{\vartheta}(s)\big)\delta(s)\Big)\Big\}\\
&+\iota\mathbb{E}\Big\{\Big(\big(\mathcal{C}_1+\tilde{\vartheta}(s)\mathcal{C}_2\big)\psi(s)+\big(\bar{\vartheta}+\tilde{\vartheta}(s)\big)\delta(s)\Big)^T\\
&\times(U^T+I)\Im\big(\zeta(s)\big)\Big\}\\
=&\mathbb{E}\Big\{\Im_1^T(s)\Psi_1\Im_1(s)\Big\}+\beta-\iota\mathbb{E}\Big\{\Im^T\big(\zeta(s)\big)\Im\big(\zeta(s)\big)\Big\}\\
&-\iota\mathbb{E}\Big\{\psi^T(s)\big(\mathcal{C}_1^T U^T\mathcal{C}_1+(\bar{\vartheta}-\bar{\vartheta}^2)\mathcal{C}_2^T U^T\mathcal{C}_2\big)\psi(s)\\
&+\bar{\vartheta}\delta^T(s)U^T\delta(s)+2\bar{\vartheta}\delta^T(s)U^T\big(\mathcal{C}_1+\mathcal{C}_2\big)\psi(s)\\
&-2\bar{\vartheta}^2\delta^T(s)U^T\mathcal{C}_2\psi(s)\Big\}+\iota\mathbb{E}\Big\{\Im^T\big(\zeta(s)\big)(U^T+I)\\
&\times\mathcal{C}_1\psi(s)+\bar{\vartheta}\delta^T(s)(U^T+I)\Im\big(\zeta(s)\big)\Big\}\\
=&\mathbb{E}\big\{\Im_2^T(s)\Psi_2\Im_2(s)\big\}+\beta
\end{aligned}\tag{29}$$

where

$$\Im_2(s)\triangleq\begin{bmatrix}\psi(s)\\ \sum_{h=1}^{\hbar}\ell_h\psi(s-h)\\ \Im\big(\zeta(s)\big)\\ \delta(s)\end{bmatrix}$$

$$\Psi_2\triangleq\begin{bmatrix}\Psi_2^{11} & \star & \star & \star\\ \Psi_1^{21} & \Psi_1^{22} & \star & \star\\ \Psi_2^{31} & \Psi_1^{32} & \Psi_2^{33} & \star\\ \Omega_1^{41} & 0 & \Omega_1^{43} & \Psi_2^{44}\end{bmatrix}$$

$$\begin{aligned}
\Psi_2^{11}\triangleq&-P+\bar{\ell}Q+\mathcal{A}^T P\mathcal{A}+\bar{\kappa}\mathcal{B}^T(s)P\mathcal{B}(s)\\
&+\sqrt{\bar{\kappa}}\mathcal{A}^T P\mathcal{B}(s)+\sqrt{\bar{\kappa}}\mathcal{B}^T(s)P\mathcal{A}\\
&-\iota\mathcal{C}_1^T U^T\mathcal{C}_1-\iota(\bar{\vartheta}-\bar{\vartheta}^2)\mathcal{C}_2^T U^T\mathcal{C}_2\\
\Psi_2^{33}\triangleq&\mathcal{F}^T P\mathcal{F}-\iota I,\quad\Psi_2^{44}\triangleq-\iota\bar{\vartheta}U^T\\
\Psi_2^{31}\triangleq&\mathcal{F}^T P\mathcal{A}+\sqrt{\bar{\kappa}}\mathcal{F}^T P\mathcal{B}(s)+\frac{1}{2}\iota(U^T+I)\mathcal{C}_1.
\end{aligned}$$

By applying the Schur Complement Lemma, we derive from (20) that

$$\Psi_2=\Omega_1+\Omega_2^T P\Omega_2<0\tag{30}$$

which further implies

$$\mathbb{E}\big\{\Re V\big(\psi(s)\big)\big\}\leqslant-\gamma\mathbb{E}\big\{\|\Im_2(s)\|^2\big\}+\beta.\tag{31}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSMC.2021.3117742, IEEE Transactions on Systems, Man, and Cybernetics: Systems.

Next, we shall proceed to estimate the upper bound of $\mathbb{E}\{\|\psi(s)\|^2\}$. Based on the definition of $V(\psi(s))$, one obtains

$$V(\psi(s)) \leqslant \lambda_{\max}(P)\|\psi(s)\|^2 + \bar{\ell}\lambda_{\max}(Q)\sum_{r=s-\hbar}^{s-1}\|\psi(r)\|^2. \tag{32}$$

Furthermore, for any $\tau > 1$, it follows from (31) that

$$\begin{aligned}
&\mathbb{E}\{\tau^{s+1}V(\psi(s+1))\} - \mathbb{E}\{\tau^s V(\psi(s))\}\\
=&\tau^{s+1}\mathbb{E}\{\Re V(\psi(s))\}+\tau^{s+1}\mathbb{E}\{V(\psi(s))\}\\
&-\tau^s\mathbb{E}\{V(\psi(s))\}\\
=&\tau^{s+1}\mathbb{E}\{\Re V(\psi(s))\}+\tau^s(\tau-1)\mathbb{E}\{V(\psi(s))\}\\
\leqslant&\tau^{s+1}\Big(-\gamma\mathbb{E}\{\|\Im_2(s)\|^2\}+\beta\Big)+\tau^s(\tau-1)\\
&\times\Big(\lambda_{\max}(P)\|\psi(s)\|^2+\bar{\ell}\lambda_{\max}(Q)\sum_{r=s-\hbar}^{s-1}\|\psi(r)\|^2\Big)\\
\leqslant&\tau^{s+1}\Big(-\gamma\mathbb{E}\{\|\psi(s)\|^2\}+\beta\Big)+\tau^s(\tau-1)\\
&\times\Big(\lambda_{\max}(P)\|\psi(s)\|^2+\bar{\ell}\lambda_{\max}(Q)\sum_{r=s-\hbar}^{s-1}\|\psi(r)\|^2\Big)\\
\leqslant&\varrho_1(\tau)\tau^s\mathbb{E}\{\|\psi(s)\|^2\}+\varrho_2(\tau)\sum_{r=s-\hbar}^{s-1}\tau^s\mathbb{E}\{\|\psi(r)\|^2\}\\
&+\tau^{s+1}\beta
\end{aligned} \tag{33}$$

where

$$\begin{aligned}
\varrho_1(\tau) &\triangleq -\tau\gamma+(\tau-1)\lambda_{\max}(P)\\
\varrho_2(\tau) &\triangleq (\tau-1)\bar{\ell}\lambda_{\max}(Q).
\end{aligned}$$

For arbitrary positive integer $\rho \geqslant \hbar$, summarizing both sides of (33) from 0 to $\rho-1$ associated with s results in

$$\begin{aligned}
&\mathbb{E}\{\tau^\rho V(\psi(\rho))\}-\mathbb{E}\{V(\psi(0))\}\\
\leqslant&\varrho_1(\tau)\sum_{s=0}^{\rho-1}\tau^s\mathbb{E}\{\|\psi(s)\|^2\}+\frac{\tau(1-\tau^\rho)}{1-\tau}\beta\\
&+\varrho_2(\tau)\sum_{s=0}^{\rho-1}\sum_{r=s-\hbar}^{s-1}\tau^s\mathbb{E}\{\|\psi(r)\|^2\}.
\end{aligned} \tag{34}$$

Besides, the last item in (34) is calculated as

$$\begin{aligned}
&\sum_{s=0}^{\rho-1}\sum_{r=s-\hbar}^{s-1}\tau^s\mathbb{E}\{\|\psi(r)\|^2\}\\
\leqslant&\left(\sum_{r=-\hbar}^{-1}\sum_{s=0}^{r+\hbar}+\sum_{r=0}^{\rho-\hbar-1}\sum_{s=r+1}^{r+\hbar}+\sum_{r=\rho-\hbar}^{\rho-1}\sum_{s=r+1}^{\rho-1}\right)\tau^s\mathbb{E}\{\|\psi(r)\|^2\}\\
\leqslant&\frac{\tau^\hbar-1}{\tau-1}\sum_{r=-\hbar}^{-1}\mathbb{E}\{\|\psi(r)\|^2\}+\frac{\tau(\tau^\hbar-1)}{\tau-1}\sum_{r=0}^{\rho-1}\tau^r\mathbb{E}\{\|\psi(r)\|^2\}\\
&+\frac{\tau(\tau^\hbar-1)}{\tau-1}\sum_{r=0}^{\rho-1}\tau^r\mathbb{E}\{\|\psi(r)\|^2\}.
\end{aligned} \tag{35}$$

From (34) and (35), one has immediately that

$$\begin{aligned}
&\mathbb{E}\{\tau^\rho V(\psi(\rho))\}-\mathbb{E}\{V(\psi(0))\}\\
\leqslant&\varrho_1(\tau)\sum_{s=0}^{\rho-1}\tau^s\mathbb{E}\{\|\psi(s)\|^2\}+\frac{\tau(1-\tau^\rho)}{1-\tau}\beta\\
&+\varrho_2(\tau)\Bigg(\frac{\tau^\hbar-1}{\tau-1}\sum_{r=-\hbar}^{-1}\mathbb{E}\{\|\psi(r)\|^2\}\\
&+\frac{\tau(\tau^\hbar-1)}{\tau-1}\sum_{r=0}^{\rho-1}\tau^r\mathbb{E}\{\|\psi(r)\|^2\}\\
&+\frac{\tau(\tau^\hbar-1)}{\tau-1}\sum_{r=0}^{\rho-1}\tau^r\mathbb{E}\{\|\psi(r)\|^2\}\Bigg)\\
\leqslant&\varrho_3(\tau)\sum_{s=0}^{\rho-1}\tau^s\mathbb{E}\{\|\psi(s)\|^2\}+\frac{\tau(1-\tau^\rho)}{1-\tau}\beta\\
&+\varrho_4(\tau)\sup_{\jmath\in\mathfrak{H}}\mathbb{E}\{\|\varphi(\jmath)\|^2\}.
\end{aligned} \tag{36}$$

where

$$\begin{aligned}
\varrho_3(\tau) &\triangleq \varrho_1(\tau)+\varrho_2(\tau)\frac{2\tau^{\hbar+1}-2\tau}{\tau-1}\\
\varrho_4(\tau) &\triangleq \varrho_2(\tau)\hbar\frac{\tau^\hbar-1}{\tau-1}.
\end{aligned}$$

Noting that $\varrho_3(1) = -\gamma < 0$ and $\lim_{\tau\to\infty}\varrho_3(\tau) = +\infty$, it is readily seen that there exists a scalar $\varepsilon > 1$ such that $\varrho_3(\varepsilon) = 0$, which indicates that

$$\begin{aligned}
&\mathbb{E}\{\varepsilon^\rho V(\psi(\rho))\}-\mathbb{E}\{V(\psi(0))\}\\
\leqslant&\frac{\varepsilon(1-\varepsilon^\rho)}{1-\varepsilon}\beta+\varrho_4(\varepsilon)\sup_{\jmath\in\mathfrak{H}}\mathbb{E}\{\|\varphi(\jmath)\|^2\}.
\end{aligned} \tag{37}$$

It can be observed from (23) that

$$\mathbb{E}\{V(\psi(0))\} \leqslant (\hbar+1)\bar{\lambda}\sup_{\jmath\in\mathfrak{H}}\mathbb{E}\{\|\varphi(\jmath)\|^2\} \tag{38}$$

and

$$\mathbb{E}\{\varepsilon^\rho V(\psi(\rho))\} \geqslant \lambda_{\min}(P)\varepsilon^\rho\mathbb{E}\{\|\psi(\rho)\|^2\}. \tag{39}$$

Furthermore, one has

$$\begin{aligned}
\mathbb{E}\{\|\psi(\rho)\|^2\} \leqslant&\frac{\varrho_4(\varepsilon)+(\hbar+1)\bar{\lambda}}{\lambda_{\min}(P)\varepsilon^\rho}\sup_{\jmath\in\mathfrak{H}}\mathbb{E}\{\|\varphi(\jmath)\|^2\}\\
&+\frac{1-\varepsilon^\rho}{\lambda_{\min}(P)\varepsilon^{\rho-1}(1-\varepsilon)}\beta\\
=&\epsilon^\rho\alpha\sup_{\jmath\in\mathfrak{H}}\mathbb{E}\{\|\varphi(\jmath)\|^2\}+\nu(\rho)
\end{aligned} \tag{40}$$

with

$$\begin{aligned}
&\epsilon \triangleq \frac{1}{\varepsilon}, \quad \alpha \triangleq \frac{\varrho_4(\varepsilon)+(\hbar+1)\bar{\lambda}}{\lambda_{\min}(P)}\\
&\nu(\rho) \triangleq \frac{1-\varepsilon^\rho}{\lambda_{\min}(P)\varepsilon^{\rho-1}(1-\varepsilon)}\beta.
\end{aligned}$$

According to Definition 1, the ultimate upper bound of the estimation error in the mean-square sense can be expressed by:

$$\bar{\nu} = \lim_{\rho\to+\infty}\nu(\rho) = \frac{\varepsilon}{\lambda_{\min}(P)(\varepsilon-1)}\beta. \tag{41}$$

To proceed, we derive from (21), (40) and (41) that

$$\mathbb{E}\{\|\psi(\rho)\|^2\} \leqslant \frac{\varrho_4(\varepsilon)+(\hbar+1)\bar{\lambda}}{\lambda_{\min}(P)\varepsilon^\rho}\sup_{\jmath\in\mathfrak{H}}\mathbb{E}\{\|\varphi(\jmath)\|^2\}$$

$$+\frac{\varepsilon}{\lambda_{\min}(P)(\varepsilon-1)}\beta\leqslant\varsigma. \tag{42}$$

Obviously, it is not difficult to see from Definition 2 that the augmented system (11) is ς-secure in mean-square sense, which ends the proof. ■

B. Outlier-Resistant PIO Design

In this subsection, we are devoted to solving the design problem of the outlier-resistant PIO.

Theorem 2: If there exist positive definite matrices $\acute{P}_1$, $\acute{P}_2$, $\acute{P}_3$, $\acute{Q}_1$, $\acute{Q}_2$ and $\acute{Q}_3$, matrices $\acute{F}_P$, $\acute{F}_I$ and $\acute{F}$, and positive scalar ι and π satisfying

$$\Lambda=\begin{bmatrix}\Omega_1 & \star\\ \Lambda_2 & \Lambda_3\end{bmatrix}<0 \tag{43}$$

and

$$\begin{aligned}&\frac{\bar{\ell}\lambda_{\max}(Q)\hbar(\varepsilon^{\hbar}-1)+(\hbar+1)\bar{\lambda}}{\lambda_{\min}(P)\varepsilon^{\rho}}\sup_{\jmath\in\mathfrak{H}}\mathbb{E}\{\|\varphi(\jmath)\|^2\}\\&+\frac{\varepsilon}{\lambda_{\min}(P)(\varepsilon-1)}\beta\leqslant\varsigma.\end{aligned} \tag{44}$$

where

$$\begin{aligned}\Lambda_2&\triangleq\begin{bmatrix}\acute{\mathcal{A}} & \acute{\mathcal{H}} & \acute{\mathcal{F}} & 0\\ 0 & 0 & 0 & 0\\ \mathcal{T} & 0 & 0 & 0\end{bmatrix}\\
\Lambda_3&\triangleq\begin{bmatrix}-P & \star & \star\\ \bar{\kappa}\mathcal{R}^T & -\pi I & \star\\ 0 & 0 & -\pi I\end{bmatrix}\\
\acute{\mathcal{A}}&\triangleq\begin{bmatrix}\acute{P}_1A & 0 & 0\\ 0 & \acute{P}_2A & -\acute{F}_I\\ 0 & 0 & \acute{P}_3\end{bmatrix}\\
\acute{\mathcal{H}}&\triangleq\begin{bmatrix}\acute{P}_1H & 0 & \\ 0 & \acute{P}_2H & 0\\ 0 & 0 & 0\end{bmatrix}\\
\acute{\mathcal{F}}&\triangleq\begin{bmatrix}0\\ -\acute{F}_P\\ \acute{F}\end{bmatrix},\quad \mathcal{R}\triangleq\begin{bmatrix}R\\ R\\ 0\end{bmatrix}\\
\mathcal{T}&\triangleq\begin{bmatrix}T & 0 & 0\end{bmatrix}\\
P&\triangleq\mathrm{diag}\{\acute{P}_1,\ \acute{P}_2,\ \acute{P}_3\}\\
Q&\triangleq\mathrm{diag}\{\acute{Q}_1,\ \acute{Q}_2,\ \acute{Q}_3\}\end{aligned}$$

and the constant $\varepsilon>1$ in (44) satisfies

$$\lambda_{\max}(P)(\varepsilon-1)-\gamma\varepsilon+2\bar{\ell}\lambda_{\max}(Q)\varepsilon(\varepsilon^{\hbar}-1)=0 \tag{45}$$

with

$$\gamma\triangleq\lambda_{\min}\big(-\Omega_1-\Omega_2^TP\Omega_2\big),$$

then the augmented system (11) is ς-secure in mean-square sense. Furthermore, the gain matrices of the outlier-resistant PIO (7) are calculated by

$$F_P=\acute{P}_1^{-1}\acute{F}_P,\quad F_I=\acute{P}_2^{-1}\acute{F}_I,\quad F=\acute{P}_3^{-1}\acute{F}. \tag{46}$$

Proof: First, we shall deal with the parameter uncertainties by rewriting (20) in the form of (19). It follows from the notations in (11) that

$$\mathcal{B}(s)=\mathcal{R}S(s)\mathcal{T}, \tag{47}$$

and therefore (20) can be rewritten as follows:

$$\Omega=\Theta_1+\Theta_RS(s)\Theta_T+\Theta_T^TS^T(s)\Theta_R^T \tag{48}$$

where

$$\begin{aligned}&\Theta_1\triangleq\begin{bmatrix}\Omega_1 & \star\\ \Theta_2 & \Omega_3\end{bmatrix},\quad \Theta_2\triangleq\begin{bmatrix}\mathcal{A} & \mathcal{H} & \mathcal{F} & 0\end{bmatrix}\\
&\Theta_R\triangleq\begin{bmatrix}0 & 0 & 0 & 0 & \bar{\kappa}\mathcal{R}^T\end{bmatrix}^T,\quad \Theta_T\triangleq\begin{bmatrix}\mathcal{T} & 0 & 0 & 0 & 0\end{bmatrix}.\end{aligned}$$

Then, by using Lemma 3, it is not difficult to see that (48) holds if and only if there exists a positive scalar π such that the following inequality holds:

$$\begin{bmatrix}\Theta_1 & \pi\Theta_R & \Theta_T^T\\ \pi\Theta_R^T & -\pi I & 0\\ \Theta_T & 0 & -\pi I\end{bmatrix}<0. \tag{49}$$

Pre-multiplying and post-multiplying the inequality (49) by $\mathrm{diag}\{I,\ I,\ I,\ I,\ P,\ I,\ I\}$ and its transpose, and utilizing the variable substitution

$$\acute{F}_P=\acute{P}_1F_P,\quad \acute{F}_I=\acute{P}_2F_I,\quad \acute{F}=\acute{P}_3F, \tag{50}$$

we conclude that (49) can be ensured by (43).

According to Theorem 1, one can conclude that, with the outlier-resistant PIO gain matrices F_P, F_P and F given in (46), the augmented system (11) is ς-secure in mean-square sense. The proof is complete. ■

C. Outlier-Resistant Luenberger Observer Design

In this subsection, we shall design an outlier-resistant Luenberger observer for system (1). To begin with, the outlier-resistant Luenberger observer is constructed as follows:

$$\begin{cases}\hat{x}(s+1)=A\hat{x}(s)+H\sum_{h=1}^{\hbar}\ell_h\hat{x}(s-h)\\ \qquad\qquad +L\Im\big(\upsilon(s)-C\hat{x}(s)\big)\\ \hat{x}(\jmath)=0,\quad\forall\jmath\in\mathfrak{H}\end{cases} \tag{51}$$

where L is the observer gain matrix to be designed.

Accordingly, from (1) and (51), the estimation error dynamics can be written as follows:

$$\begin{cases}\tilde{x}(s+1)=A\tilde{x}(s)+H\sum_{h=1}^{\hbar}\ell_h\tilde{x}(s-h)+Mw(s)\\ \qquad\qquad +\kappa(s)B(s)x(s)-L\Im\big(\upsilon(s)-C\hat{x}(s)\big)\\ \tilde{x}(\jmath)=\phi(\jmath),\quad\forall\jmath\in\mathfrak{H}\end{cases} \tag{52}$$

Letting $\breve{\psi}(s)\triangleq\begin{bmatrix}x^T(s) & \tilde{x}^T(s)\end{bmatrix}^T$, the augmented system is characterized as follows:

$$\begin{cases}\breve{\psi}(s+1)=\big(\breve{\mathcal{A}}+\bar{\kappa}\breve{\mathcal{B}}(s)+\tilde{\kappa}(s)\breve{\mathcal{B}}(s)\big)\breve{\psi}(s)\\ \qquad\qquad +\breve{\mathcal{H}}\sum_{h=1}^{\hbar}\ell_h\breve{\psi}(s-h)+\breve{\mathcal{M}}w(s)\\ \qquad\qquad +\breve{\mathcal{F}}\Im\big(\breve{\zeta}(s)\big)\\ \breve{\psi}(\jmath)=\breve{\varphi}(\jmath),\quad\forall\jmath\in\mathfrak{H}\end{cases} \tag{53}$$

where

$$\breve{\mathcal{A}}\triangleq\begin{bmatrix}A & 0\\ 0 & A\end{bmatrix},\quad \breve{\mathcal{H}}\triangleq\begin{bmatrix}H & 0\\ 0 & H\end{bmatrix}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSMC.2021.3117742, IEEE Transactions on Systems, Man, and Cybernetics: Systems.

$$\breve{\mathcal{B}}(s) \triangleq \begin{bmatrix} B(s) & 0 \\ B(s) & 0 \end{bmatrix}, \quad \breve{\mathcal{M}} \triangleq \begin{bmatrix} M \\ M \end{bmatrix}$$
$$\breve{\mathcal{F}} \triangleq \begin{bmatrix} 0 \\ -L \end{bmatrix}, \quad \breve{\mathcal{C}}_1 \triangleq \begin{bmatrix} -\bar{\vartheta}C & C \end{bmatrix}$$
$$\breve{\mathcal{C}}_2 \triangleq \begin{bmatrix} -C & 0 \end{bmatrix}, \quad \breve{\varphi}(\jmath) \triangleq \begin{bmatrix} \phi^T(\jmath) & \phi^T(\jmath) \end{bmatrix}^T$$
$$\breve{\zeta}(s) \triangleq \big(\mathcal{C}_1 + \tilde{\vartheta}(s)\mathcal{C}_2\big)\breve{\psi}(s) + \big(\bar{\vartheta} + \tilde{\vartheta}(s)\big)\delta(s).$$

In the following corollary, sufficient conditions are provided to a) ensure that the augmented system (53) is ς-secure in mean-square sense and b) give an explicit form of the gain matrix of outlier-resistant Luenberger observer (51) by means of LMI technique.

Corollary 1: If there exist positive definite matrices $\grave{P}_1$, $\grave{P}_2$, $\grave{Q}_1$ and $\grave{Q}_2$, matrix $\grave{L}$, and positive scalar $\breve{\iota}$ and $\breve{\pi}$ satisfying

$$\Xi = \begin{bmatrix} \Xi_1 & \star \\ \Xi_2 & \Xi_3 \end{bmatrix} < 0 \tag{54}$$

and

$$\frac{\bar{\ell}\lambda_{\max}(\breve{Q})\hbar(\breve{\varepsilon}^{\hbar}-1)+(\hbar+1)\breve{\lambda}}{\lambda_{\min}(\breve{P})\varepsilon^{\rho}}\sup_{\jmath\in\mathfrak{H}}\mathbb{E}\{\|\breve{\varphi}(\jmath)\|^2\} + \frac{\breve{\varepsilon}}{\lambda_{\min}(\breve{P})(\breve{\varepsilon}-1)}\breve{\beta} \leqslant \varsigma. \tag{55}$$

where

$$\Xi_1 \triangleq \begin{bmatrix} \Xi_1^{11} & \star & \star & \star \\ 0 & \Xi_1^{22} & \star & \star \\ \Xi_1^{31} & 0 & \Xi_1^{33} & \star \\ \Xi_1^{41} & 0 & \Xi_1^{43} & \Xi_1^{44} \end{bmatrix}, \ \Xi_2 \triangleq \begin{bmatrix} \grave{\mathcal{A}} & \grave{\mathcal{H}} & \grave{\mathcal{F}} & 0 \\ 0 & 0 & 0 & 0 \\ \breve{\mathcal{T}} & 0 & 0 & 0 \end{bmatrix}$$
$$\Xi_3 \triangleq \begin{bmatrix} -\breve{P} & \star & \star \\ \bar{\kappa}\breve{\mathcal{R}}^T & -\breve{\pi}I & \star \\ 0 & 0 & -\breve{\pi}I \end{bmatrix}, \quad \breve{\beta} \triangleq \lambda_{\max}(\breve{\mathcal{M}}^T\breve{P}\breve{\mathcal{M}})\vartheta_w^2$$
$$\grave{\mathcal{A}} \triangleq \begin{bmatrix} \grave{P}_1 A & 0 \\ 0 & \grave{P}_2 A \end{bmatrix}, \quad \breve{P} \triangleq \text{diag}\{\grave{P}_1,\ \grave{P}_2\}$$
$$\grave{\mathcal{H}} \triangleq \begin{bmatrix} \grave{P}_1 H & 0 \\ 0 & \grave{P}_2 H \end{bmatrix}, \quad \breve{Q} \triangleq \text{diag}\{\grave{Q}_1,\ \grave{Q}_2\}$$
$$\grave{\mathcal{F}} \triangleq \begin{bmatrix} 0 \\ -\grave{L} \end{bmatrix}, \quad \breve{\mathcal{R}} \triangleq \begin{bmatrix} R \\ R \end{bmatrix}, \quad \breve{\mathcal{T}} \triangleq \begin{bmatrix} T & 0 \end{bmatrix}$$
$$\Xi_1^{11} \triangleq -\breve{P} + \bar{\ell}\breve{Q} - \breve{\iota}\breve{\mathcal{C}}_1^T U^T \breve{\mathcal{C}}_1 - \breve{\iota}(\bar{\vartheta} - \bar{\vartheta}^2)\breve{\mathcal{C}}_2^T U^T \breve{\mathcal{C}}_2$$
$$\Xi_1^{22} \triangleq -\frac{1}{\bar{\ell}}\breve{Q}, \quad \Xi_1^{33} \triangleq -\breve{\iota}I, \quad \Xi_1^{44} \triangleq -\breve{\iota}\bar{\vartheta}U^T$$
$$\Xi_1^{31} \triangleq \frac{1}{2}\breve{\iota}(U^T + I)\breve{\mathcal{C}}_1, \quad \Xi_1^{41} \triangleq -\breve{\iota}\bar{\vartheta}U^T\big(\breve{\mathcal{C}}_1 + \breve{\mathcal{C}}_2 - \bar{\vartheta}\breve{\mathcal{C}}_2\big)$$
$$\Xi_1^{43} \triangleq \frac{1}{2}\breve{\iota}\bar{\vartheta}(U^T + I), \quad \breve{\lambda} \triangleq \max\{\lambda_{\max}(\breve{P}),\ \bar{\ell}\lambda_{\max}(\breve{Q})\}$$

and the constant $\breve{\varepsilon} > 1$ in (55) satisfies

$$\lambda_{\max}(\breve{P})(\breve{\varepsilon}-1) - \breve{\gamma}\breve{\varepsilon} + 2\bar{\ell}\lambda_{\max}(\breve{Q})\breve{\varepsilon}(\breve{\varepsilon}^{\hbar}-1) = 0 \tag{56}$$

with

$$\breve{\gamma} \triangleq \lambda_{\min}\big(-\Xi_1 - \Xi_3^T\breve{P}\Xi_3\big)$$
$$\Xi_3 \triangleq \begin{bmatrix} \breve{\mathcal{A}} + \bar{\kappa}\breve{\mathcal{B}}(s) & \breve{\mathcal{H}} & \breve{\mathcal{F}} & 0 \end{bmatrix},$$

then the augmented system (53) is ς-secure in mean-square sense. Furthermore, the gain matrix of the outlier-resistant Luenberger observer (51) is calculated by

$$L = \grave{P}_2^{-1}\grave{L}. \tag{57}$$

Proof: The proof of this corollary is easily obtained only by setting $F_I = 0$ and $F = 0$ in Theorems 1-2, and is therefore omitted here. ∎

Remark 4: Up to now, we have thoroughly investigated the outlier-resistant PIO design issue for a kind of discrete-time delayed system with ROPUs subject to RODAs. With the designed outlier-resistant PIO, the EMS boundedness of the estimation errors has been guaranteed and the security requirement has been met. In addition, the feasibility of the PIO design problem has been transformed into the solvability of an LMI. In comparison with the existing literature, our main results exhibit the following distinctive novelties: 1) the PIO design problem is, for the first time, addressed for discrete time-delayed systems with RODAs; 2) the outlier-resistant PIO design scheme is developed to attenuate the effect of malicious attacks; and 3) a criterion is derived to reveal the influences of the RODAs and the stochastic noise on the estimation performance. Our main results can be extended to more complicated NSs with more comprehensive network-induced phenomena or cyber-attacks [18], [43].

IV. Numerical Simulation

In this section, an illustrative example is provided to show the effectiveness and superiority of the proposed outlier-resistant PIO design scheme.

Consider a linear discrete time-delayed system described by (1) with the following parameters:

$$A = \begin{bmatrix} 0.46 & 0.92 \\ -0.44 & 0.61 \end{bmatrix}, \quad H = \begin{bmatrix} 0.11 & 0.14 \\ 0.15 & -0.13 \end{bmatrix}$$
$$C = \begin{bmatrix} -0.72 & 0.61 \end{bmatrix}, \quad D = \begin{bmatrix} 1.1 & 0.9 \end{bmatrix}, \quad U = 0.35$$
$$M = \begin{bmatrix} -0.06 \\ 0.11 \end{bmatrix}, \ R = \begin{bmatrix} 0.6 \\ 0.5 \end{bmatrix}, \ T = \begin{bmatrix} 0.2 \\ 0.3 \end{bmatrix}^T, \ \bar{\kappa} = 0.3$$
$$\hbar = 3, \quad \ell_h = 2^{-(h+1)}, \quad S(s) = 0.8\sin(s).$$

A. Effectiveness and Superiority of the Proposed Outlier-Resistant PIO Design Approach

In the simulation, the deception signal sent by adversary is denoted by $\delta(s) = 5\cos(s) - \tanh(s)$ and the probability of launching a successful deception attack is given as $\bar{\vartheta} = 0.4$. In addition, the security level is selected as $\varsigma = 0.2$ and the initial condition is taken as $x(0) = \begin{bmatrix} 0.5 & -0.5 \end{bmatrix}^T$.

The solutions to LMI (43) in Theorem 2 are obtained as follows:

$$\acute{P}_1 = \begin{bmatrix} 9.5817 & -1.6386 \\ -1.6386 & 16.8731 \end{bmatrix}, \ \acute{Q}_1 = \begin{bmatrix} 1.6118 & -0.0089 \\ -0.0089 & 1.6029 \end{bmatrix}$$
$$\acute{P}_2 = \begin{bmatrix} 9.3057 & -1.5956 \\ -1.5956 & 20.3154 \end{bmatrix}, \ \acute{Q}_2 = \begin{bmatrix} 1.6421 & -0.0241 \\ -0.0241 & 1.5996 \end{bmatrix}$$
$$\acute{P}_3 = 8.7174, \ \acute{Q}_3 = 2.2466, \ \acute{F} = -0.0090, \ \pi = 1.2797$$
$$\acute{F}_P = \begin{bmatrix} -0.6424 \\ 3.5330 \end{bmatrix}, \quad \acute{F}_I = \begin{bmatrix} -0.3534 \\ 0.5101 \end{bmatrix}, \quad \iota = 1.3848.$$

Accordingly, the outlier-resistant PIO gains can be computed as follows:

$$F_P = \begin{bmatrix} -0.0318 \\ 0.2063 \end{bmatrix}, \quad F_I = \begin{bmatrix} 0.0429 \\ 0.0285 \end{bmatrix}, \quad \acute{F} = -0.0010.$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSMC.2021.3117742, IEEE Transactions on Systems, Man, and Cybernetics: Systems.

Furthermore, according to Corollary 1, the solutions of LMI (54) and the gain of outlier-resistant Luenberger observer (51) are listed as follows:

$$\grave{P}_1 = \begin{bmatrix} 4.4852 & -0.6864 \\ -0.6864 & 7.1213 \end{bmatrix}, \ \grave{Q}_1 = \begin{bmatrix} 0.6057 & -0.0033 \\ -0.0033 & 0.6071 \end{bmatrix}$$

$$\grave{P}_2 = \begin{bmatrix} 4.3151 & -0.5025 \\ -0.5025 & 7.2158 \end{bmatrix}, \ \grave{Q}_2 = \begin{bmatrix} 0.6057 & -0.0034 \\ -0.0034 & 0.6063 \end{bmatrix}$$

$$\grave{L} = \begin{bmatrix} -0.0275 \\ 2.3519 \end{bmatrix}, \ L = \begin{bmatrix} 0.0318 \\ 0.3282 \end{bmatrix}, \ \breve{\pi} = 7.5951, \ \breve{\iota} = 6.9122.$$

For manifesting the superiority of the outlier-resistant PIO, we make comparisons for evaluating the estimation performance under different observers as follows: 1) estimating with the outlier-resistant PIO; 2) estimating with the outlier-resistant Luenberger observer; 3) estimating with the conventional PIO (which corresponds to $l^M = \infty$).

The estimation results are shown in Figs. 1-2, which depict the system states and their estimates with different observers. From Figs. 1-2, we observe that the outlier-resistant Luenberger observer and the conventional PIO cannot achieve the desired estimation performance whereas the outlier-resistant PIO can. Figs. 3-5 plot the trajectories of estimation error $\tilde{x}(s)$ with the outlier-resistant PIO, the outlier-resistant Luenberger observer, and the conventional PIO, respectively.

From the above simulation results, a conclusion can be drawn that the outlier-resistant PIO is able to mitigate the negative effects of the RODAs and achieve a satisfactory estimation performance. Consequently, the design scheme of the developed outlier-resistant PIO is indeed efficient and performs better than the outlier-resistant Luenberger observer and the conventional PIO.

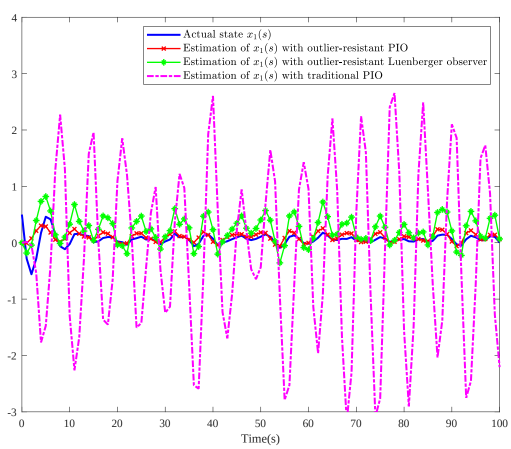


Fig. 1: Trajectories of state $x_1(s)$ and its estimate.

B. Comparisons With Different Attack Probabilities

For the sake of truly revealing the impact from the RODAs on our estimation algorithm, the simulations are repeated 100 times and the comparisons with different attack probabilities are made in this subsection. To facilitate discussion, the

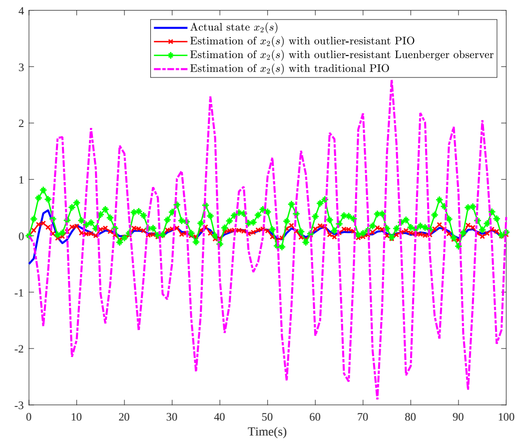


Fig. 2: Trajectories of state $x_2(s)$ and its estimate.

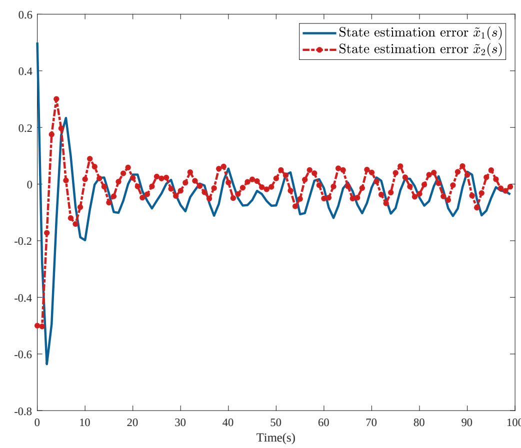


Fig. 3: Trajectories of estimation error $\tilde{x}(s)$ with outlier-resistant PIO.

average mean-square estimation error (AMSEE) with respect to the output is defined by:

$$\mathcal{Z} = \frac{1}{p}\sum_{s=1}^{p}\frac{1}{q}\sum_{\imath=1}^{q}\|z^{\imath}(s) - \hat{z}^{\imath}(s)\|^2$$

where p denotes the number of time instants and q stands for the number of simulation trials.

Fig. 6 depicts the trajectories of measurement output $y(s)$, observer input $\upsilon(s)$, and the time spots when the system suffers from deception attacks with $\bar{\vartheta} = 0.4$. Moreover, the relation between the attack probability $\bar{\vartheta}$ and the AMSEE of the estimated output $\mathcal{Z}$ is given in Table I, which can be observed that the AMSEE of the output increases when the attack probability increases. Therefore, we can naturally draw a conclusion that, with the increase of the attack probability, the estimation performance deteriorates.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSMC.2021.3117742, IEEE Transactions on Systems, Man, and Cybernetics: Systems.

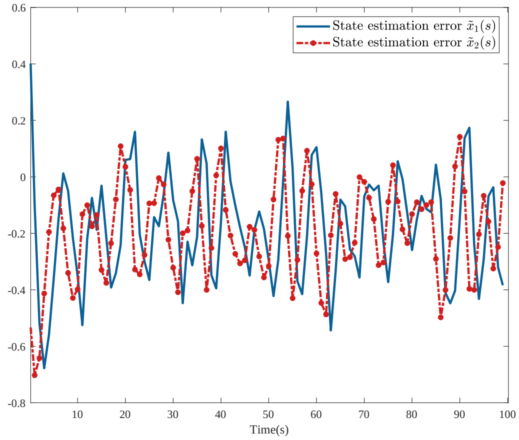


Fig. 4: Trajectories of estimation error $\tilde{x}(s)$ with outlier-resistant Luenberger observer.

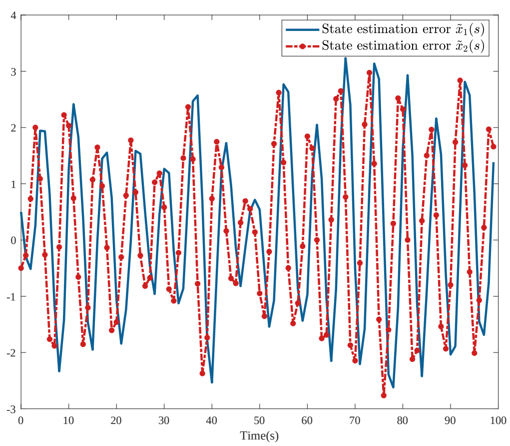


Fig. 5: Trajectories of estimation error $\tilde{x}(s)$ with conventional PIO.

V. Conclusions

In this paper, the PIO design issue has been addressed for a kind of discrete-time delayed system with ROPUs subject to RODAs. A Bernoulli-distributed random variable has been utilized to regulate the random nature of deception attacks initiated by the adversaries. For the purpose of attenuating the impact of the malicious attacks on the estimation performance, an outlier-resistant PIO has been constructed, in which a saturation constraint has been imposed on the innovations. Sufficient conditions have been derived to guarantee the EMS boundedness and achieve the prescribed security level. The explicit forms of the desired PIO parameters have been described in terms of the solutions to an LMI. Finally, the effectiveness and superiority have been validated via an illustrative simulation example.

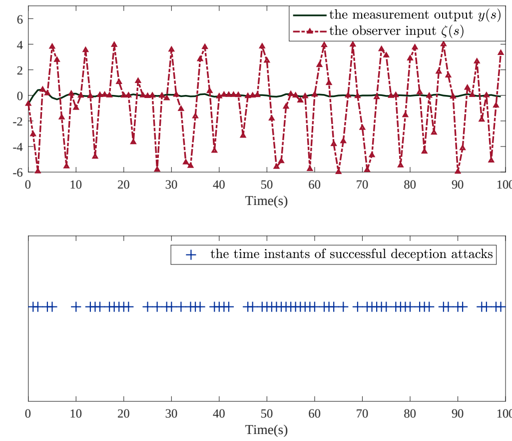


Fig. 6: The trajectories of measurement output $y(s)$ and observer input $v(s)$, and the time instants of successful deception attacks with $\bar{\vartheta} = 0.4$.

TABLE I: AMSEE IN 100 EXPERIMENTS WITH DIFFERENT $\bar{\vartheta}$

$\bar{\vartheta}$	$\mathcal{Z}$
$\bar{\vartheta} = 0.1$	0.0191
$\bar{\vartheta} = 0.2$	0.0205
$\bar{\vartheta} = 0.3$	0.0229
$\bar{\vartheta} = 0.4$	0.0233
$\bar{\vartheta} = 0.5$	0.0255
$\bar{\vartheta} = 0.6$	0.0261
$\bar{\vartheta} = 0.7$	0.0286
$\bar{\vartheta} = 0.8$	0.0326
$\bar{\vartheta} = 0.9$	0.0372

References

[1] A. Alessandri and M. Awawdeh, Moving-horizon estimation with guaranteed robustness for discrete-time linear systems and measurements subject to outliers, *Automatica*, vol. 67, pp. 85–93, May 2016.

[2] A. Alessandri and L. Zaccarian, Stubborn state observers for linear timeinvariant systems, *Automatica*, vol. 88, pp. 1–9, Feb. 2018.

[3] F. Bakhshande and D. Söffker, Proportional-integral-observer: A brief survey with special attention to the actual methods using acc benchmark, *IFAC-PapersOnLine*, vol. 48, no. 1, pp. 532–537, Jun. 2015.

[4] M. V. Basin, A. G. Loukianov and M. Hernandez-Gonzalez, Joint state and parameter estimation for uncertain stochastic nonlinear polynomial systems, *International Journal of Systems Science*, vol. 44, no. 7, pp. 1200–1208, Jul. 2013.

[5] S. Beale and B. Shafai, Robust control system design with a proportional integral observer, *International Journal of Control*, vol. 50, no. 1, pp. 97–111, Apr. 1989.

[6] G. K. Befekadu, V. Gupta and P. J. Antsaklis, Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies, *IEEE Transactions on Automatic Control*, vol. 60, no. 12, pp. 3299–3304, Dec. 2015.

[7] R. Caballero-Águila, A. Hermoso-Carazo and J. Linares-Pérez, Distributed fusion filters from uncertain measured outputs in sensor networks with random packet losses, *Information Fusion*, vol. 34, pp. 70–79, Mar. 2017.

[8] A. Cetinkaya, H. Ishii and T. Hayakawa, Networked control under random and malicious packet losses, *IEEE Transactions on Automatic Control*, vol. 62, no. 5, pp. 2434–2449, May 2017.

[9] J.-L. Chang, Applying discrete-time proportional integral observers for

state and disturbance estimations, *IEEE Transactions on Automatic Control*, vol. 51, no. 5, pp. 814–818, May 2006.

[10] D. Ciuonzo, A. Aubry and V. Carotenuto, Rician MIMO channel- and jamming-aware decision fusion, *IEEE Transactions on Signal Processing*, vol. 65, no. 15, pp. 3866–3880, Aug. 2017.

[11] Y. Cui, Y. Liu, W. Zhang and F. E. Alsaadi, Sampled-based consensus for nonlinear multiagent systems with deception attacks: The decoupled method, *IEEE Transactions on Systems, Man and Cybernetics: Systems*, vol. 51, no. 1, pp. 561–573, Jan. 2021.

[12] J. Dai and H. C. So, Sparse Bayesian learning approach for outlier-resistant direction-of-arrival estimation, *IEEE Transactions on Signal Processing*, vol. 66, no. 3, pp. 744–756, Feb. 2018.

[13] H. Dong, J. Lam and H. Gao, Distributed H_∞ filtering for repeated scalar nonlinear systems with random packet losses in sensor networks, *International Journal of Systems Science*, vol. 42, no. 9, pp. 1507–1519, Sept. 2011.

[14] H. Fu, H. Dong, F. Han, Y. Shen and N. Hou, Outlier-resistant H_∞ filtering for a class of networked systems under Round-Robin protocol, *Neurocomputing*, vol. 403, pp. 133–142, Aug. 2020.

[15] X. Ge, Q.-L. Han, X.-M. Zhang, L. Ding and F. Yang, Distributed event-triggered estimation over sensor networks: A survey, *IEEE Transactions on Cybernetics*, vol. 50, no. 3, pp. 1306–1320, Mar. 2020.

[16] R. Gibbs, New Kalman filter and smoother consistency tests, *Automatica*, vol. 49, pp. 3141–3144, Oct. 2013.

[17] W. He, F. Qian, Q.-L. Han and G. Chen, Almost sure stability of nonlinear systems under random and impulsive sequential attacks, *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3879–3886, Sep. 2020.

[18] Y. Ju, Y. Liu, X. He and B. Zhang, Finite-horizon H_∞ filtering and fault isolation for a class of time-varying systems with sensor saturation, *International Journal of Systems Science*, vol. 52, no. 2, pp. 321–333, Oct. 2021.

[19] H. R. Karimi, Robust H_∞ filter design for uncertain linear systems over network with network-induced delays and output quantization, *Modeling Identification and Control*, vol. 30, no. 1, pp. 27–37, 2009.

[20] H. R. Karimi and H. Gao, New delay-dependent exponential H_∞ synchronization for uncertain neural networks with mixed time delays, *IEEE Transactions on Systems, Man, and Cybernetics, Part B-Cybernetics*, vol. 40, no. 1, pp. 173–185, Feb. 2010.

[21] K.-S. Kim, K.-H. Rew and S. Kim, Disturbance observer for estimating higher order disturbances in time series expansion, *IEEE Transactions on Automatic Control*, vol. 55, no. 8, pp. 1905–1911, Aug. 2010.

[22] D. Koenig, Unknown input proportional multiple-integral observer design for linear descriptor systems: Application to state and fault estimation, *IEEE Transactions on Automatic Control*, vol. 50, no. 2, pp. 212–217, Feb. 2005.

[23] Y. Li, L. Shi, P. Cheng, J. Chen and D. E. Quevedo, Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach, *IEEE Transactions on Automatic Control*, vol. 60, no. 10, pp. 2831–2836, Oct. 2015.

[24] L. Liu, L. Ma, J. Zhang and Y. Bo, Distributed non-fragile set-membership filtering for nonlinear systems under fading channels and bias injection attacks, *International Journal of Systems Science*, vol. 52, no. 6, pp. 1192–1205, Jan. 2021.

[25] T. Liu and J. Huang, Robust output regulation of discrete-time linear systems by quantized output feedback control, *Automatica*, vol. 107, pp. 587–590, Sept. 2019.

[26] Y. Liu, H. Wang and L. Guo, Composite robust H_∞ control for uncertain stochastic nonllinear systems with state delay via a disturbance observer, *IEEE Transactions on Automatic Control*, vol. 63, no. 12, pp. 4345–4352, Dec. 2018.

[27] J. Mao, D. Ding, G. Wei and H. Liu, Networked recursive filtering for time-delayed nonlinear stochastic systems with uniform quantisation under Round-Robin protocol, *International Journal of Systems Science*, vol. 50, no. 4, pp. 871–884, Mar. 2019.

[28] H. Meng, H. Zhang, Z. Wang and G. Cheng, Event-triggered control for semiglobal robust consensus of a class of nonlinear uncertain multiagent systems, *IEEE Transactions on Automatic Control*, vol. 65, no. 4, pp. 1683–1690, Apr. 2020.

[29] Y. Mo and B. Sinopoli, On the performance degradation of cyber-physical systems under stealthy integrity attacks, *IEEE Transactions on Automatic Control*, vol. 61, no. 9, pp. 2618–2624, Sept. 2016.

[30] H.-Q. Mu and K.-V. Yuen, Novel outlier-resistant extended Kalman filter for robust online structural identification, *Journal of Engineering Mechanics*, vol. 141, no. 1, Art. no. 04014100, Jan. 2015.

[31] H. H. Niemann, J. Stoustrup, B. Shafai and S. Beale, LTR design of proportional-integral observers, *International Journal of Robust and Nonlinear Control*, vol. 5, no. 7, pp. 671–693, 1995.

[32] L. Peng, L. Shi, X. Cao and C. Sun, Optimal attack energy allocation against remote state estimation, *IEEE Transactions on Automatic Control*, vol. 63, no. 7, pp. 2199–2205, Jul. 2018.

[33] B. Shafai, S. Beale, H. H. Niemann and J. L. Stoustrup, LTR design of discrete-time proportional-integral observers, *IEEE Transactions on Automatic Control*, vol. 41, no. 7, pp. 1056–1062, Jul. 1996.

[34] D. Söffker, T. J. Yu and P. C. Müller, State estimation of dynamical systems with nonlinearities by using proportional-integral observer, *International Journal of Systems Science*, vol. 26, no. 9, pp. 1571–1582, Nov. 1995.

[35] H. Song, D. Ding, H. Dong, G. Wei and Q.-L. Han, Distributed entropy filtering subject to DoS attacks in non-Gauss environments, *International Journal of Robust and Nonlinear Control*, vol. 30, no. 3, pp. 1240–1257, Jan. 2020.

[36] H. Song, D. Ding, H. Dong, G. Wei and Q.-L. Han, Distributed entropy filtering subject to DoS attacks in non-Gauss environments, *International Journal of Robust and Nonlinear Control*, vol. 30, no. 3, pp. 1240–1257, Feb. 2020.

[37] T. Tian, S. Sun and N. Li, Multi-sensor information fusion estimators for stochastic uncertain systems with correlated noises, *Information Fusion*, vol. 27, pp. 126–137, Jan. 2016.

[38] D. F. Vecchia and J. D. Splett, Outlier-resistant methods for estimation and model fitting, *ISA Transactions*, vol. 33, no. 4, pp. 411–420, Dec. 1994.

[39] Y. Wang, L. Zou, Z. Zhao and X. Bai, H_∞ fuzzy PID control for discrete time-delayed TS fuzzy systems, *Neurocomputing*, vol. 332, pp. 91–99, Mar. 2019.

[40] B. Wojciechowski, Analysis and synthesis of proportional-intergral observers for single-input single-output time-invariant continuous systems, *Ph. D. Thesis, Gliwice, Poland*, 1978.

[41] S. Xiao, Q.-L. Han, X. Ge and Y. Zhang, Secure distributed finite-time filtering for positive systems over sensor networks under deception attacks, *IEEE Transactions on Cybernetics*, vol. 50, no. 3, pp. 1220–1229, Mar. 2020.

[42] W. Xu, G. Hu, D. W. C. Ho and Z. Feng, Distributed secure cooperative control under denial-of-service attacks from multiple adversaries, *IEEE Transactions on Cybernetics*, vol. 50, no. 8, pp. 3458–3467, Aug. 2020.

[43] Y. Xu, R. Lu, P. Shi, H. Li and S. Xie, Finite-time distributed state estimation over sensor networks with round-robin protocol and fading channels, *IEEE Transactions on Cybernetics*, vol. 48, no. 1, pp. 336–345, Jan. 2018.

[44] Y. Yu and Y. Yuan, Event-triggered active disturbance rejection control for nonlinear network control systems subject to DoS and physical attacks, *ISA Transactions*, DOI: 10.1016/j.isatra.2019.05.004.

[45] X.-M. Zhang, Q.-L. Han and X. Ge, A novel finite-sum inequality-based method for robust H_∞ control of uncertain discrete-time Takagi-Sugeno fuzzy systems with interval-like time-varying delays, *IEEE Transactions on Cybernetics*, vol. 48, no. 9, pp. 2569–2582, Sept. 2018.

[46] G. Zhang and Y. Shen, New algebraic criteria for synchronization stability of chaotic memristive neural networks with time-varying delays, *IEEE Transactions on Neural Networks and Learning Systems*, vol. 24, no. 10, pp. 1701–1707, Oct. 2013.

[47] M. Zhu and S. Martínez, On the performance analysis of resilient networked control systems under replay attacks, *IEEE Transactions on Automatic Control*, vol. 59, no. 3, pp. 804–808, Mar. 2014.

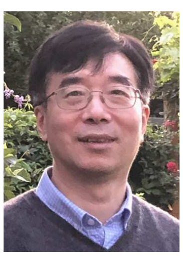
[48] W. Zhu, J. Tang, S. Wan and J. L. Zhu, Outlier-resistant adaptive filtering based on sparse Bayesian learning, *Electronics Letters*, vol. 50, no. 9, pp. 663–665, Apr. 2014

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TSMC.2021.3117742, IEEE Transactions on Systems, Man, and Cybernetics: Systems.

Di Zhao received the B.Sc. degree in Mathematics from Jilin Normal University, Siping, China, in 2013 and the Ph.D. degree in Control Science and Engineering from University of Shanghai for Science and Technology, Shanghai, China, in 2020. She is currently a Postdoctoral Research Fellow with the College of Science, University of Shanghai for Science and Technology, Shanghai, China.

From November 2018 to November 2019, she was a visiting Ph.D. student in the Department of Computer Science, Brunel University London, Uxbridge, U.K.. From March to June 2018, she was a Research Associate in the Department of Mathematics, City University of Hong Kong, Hong Kong.

Dr. Zhao's research interests include PID control, proportional-integral observer, networked control systems and cyber-physical systems. She is currently a reviewer for some international journals.



Zidong Wang (Fellow, IEEE) was born in Jiangsu, China, in 1966. He received the B.Sc. degree in mathematics in 1986 from Suzhou University, Suzhou, China, and the M.Sc. degree in applied mathematics in 1990 and the Ph.D. degree in electrical engineering in 1994, both from Nanjing University of Science and Technology, Nanjing, China.

He is currently Professor of Dynamical Systems and Computing in the Department of Computer Science, Brunel University London, U.K. From 1990 to 2002, he held teaching and research appointments in universities in China, Germany and the UK. Prof. Wang's research interests include dynamical systems, signal processing, bioinformatics, control theory and applications. He has published more than 600 papers in international journals. He is a holder of the Alexander von Humboldt Research Fellowship of Germany, the JSPS Research Fellowship of Japan, William Mong Visiting Research Fellowship of Hong Kong.

Prof. Wang serves (or has served) as the Editor-in-Chief for *International Journal of Systems Science*, the Editor-in-Chief for *Neurocomputing*, the Editor-in-Chief for *Systems Science & Control Engineering*, and an Associate Editor for 12 international journals including IEEE Transactions on Automatic Control, IEEE Transactions on Control Systems Technology, IEEE Transactions on Neural Networks, IEEE Transactions on Signal Processing, and IEEE Transactions on Systems, Man, and Cybernetics-Part C. He is a Member of the Academia Europaea, a Member of the European Academy of Sciences and Arts, an Academician of the International Academy for Systems and Cybernetic Sciences, a Fellow of the IEEE, a Fellow of the Royal Statistical Society and a member of program committee for many international conferences.

Qing-Long Han (Fellow, IEEE) received the B.Sc. degree in Mathematics from Shandong Normal University, Jinan, China, in 1983, and the M.Sc. and Ph.D. degrees in Control Engineering from East China University of Science and Technology, Shanghai, China, in 1992 and 1997, respectively.

Prof. Han is Pro Vice-Chancellor (Research Quality) and a Distinguished Professor at Swinburne University of Technology, Melbourne, Australia. He held various academic and management positions at Griffith University and Central Queensland University, Australia. His research interests include networked control systems, multi-agent systems, time-delay systems, smart grids, unmanned surface vehicles, and neural networks.

Prof. Han was a Highly Cited Researcher in both Engineering and Computer Science (Clarivate Analytics). He was one of Australia's Top 5 Lifetime Achievers (Research Superstars) in Engineering and Computer Science (The Australian's Research Magazine, 2019-2020). He was the recipient of The 2021 M. A. Sargent Medal (the Highest Award of the Electrical College Board of Engineers Australia), The 2020 IEEE Systems, Man, and Cybernetics (SMC) Society Andrew P. Sage Best Transactions Paper Award, The 2020 IEEE Transactions on Industrial Informatics Outstanding Paper Award, and The 2019 IEEE SMC Society Andrew P. Sage Best Transactions Paper Award.

Prof. Han is a Member of the Academia Europaea (The Academy of Europe) and a Fellow of The Institution of Engineers Australia. He has served as an AdCom Member of IEEE Industrial Electronics Society (IES), a Member of IEEE IES Fellow Committee, and Chair of IEEE IES Technical Committee on Networked Control Systems. He is Co-Editor-in-Chief of IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, Co-Editor of Australian Journal of Electrical and Electronic Engineering, an Associate Editor for 12 international journals, including the IEEE TRANSACTIONS ON CYBERNETICS, the IEEE INDUSTRIAL ELECTRONICS MAGAZINE, the IEEE/CAA JOURNAL OF AUTOMATICA SINICA, Control Engineering Practice, and Information Sciences, and a Guest Editor for 13 Special Issues.

Guoliang Wei received the B.Sc. degree in mathematics from Henan Normal University, Xinxiang, China, in 1997, and the M.Sc. degree in applied mathematics and the Ph.D. degree in control engineering from Donghua University, Shanghai, China, in 2005 and 2008, respectively.

He is currently a Professor with the College of Science, University of Shanghai for Science and Technology, Shanghai. From March 2010 to May 2011, he was an Alexander von Humboldt Research Fellow with the Institute for Automatic Control and Complex Systems, University of Duisburg-Essen, Duisburg, Germany. From March 2009 to February 2010, he was a Postdoctoral Research Fellow with the Department of Information Systems and Computing, Brunel University, Uxbridge, U.K., sponsored by the Leverhulme Trust of the U.K. From June 2007 to August 2007, he was a Research Assistant with the University of Hong Kong, Hong Kong. From March 2008 to May 2008, he was a Research Assistant with the City University of Hong Kong, Hong Kong. He has published more than 100 papers in refereed international journals. His research interests include nonlinear systems, stochastic systems, and bioinformatics.

Prof. Wei is a very active reviewer for many international journals.